ABSTRACT OF THE DISCLOSURE

A random number generator comprising an oscillator with an output signal dependant upon a random source, a sampling device to sample the output signal from the oscillator to obtain a sampled oscillator output, and a fixed frequency clock driven linear feedback shift register (LFSR) communicatively coupled to the sampling device via a digital gate to receive the sampled oscillator output, and to provide a random number at an output of the LFSR. Additionally, the random number generator may comprise an optional mixing function communicatively coupled to the LFSR to read the random number, and to insert the random number into an algorithm to obtain a robust random number.

A method and apparatus to implement the mixing function comprising a processor to read a seed from an entropy generator, to modify the seed, to insert the modified seed into a mixing function, to initialize a set of input variables used in the mixing function to generate a robust random number, and to generate subsequent robust random numbers using the mixing function without re-initializing any of the set of input variables.